FINAL REPORT

To

The Florida Department of Transportation
Research Center

On Project

"Development of Automated Testing Tools for Traffic Control Signals and Devices (NTCIP and Security) Phase 2"

FDOT Contract Number BDV30-977-05

February 2, 2015

By

Leonard J. Tung
Department of Electrical and Computer Engineering
FAMU-FSU College of Engineering, Florida State University

DISCLAIMER

The opinions, findings, and conclusions expressed in this publication are those of the authors and not necessarily those of the State of Florida Department of Transportation.

TECHNICAL REPORT DOCUMENTATION PAGE

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle *Development of Automated Testing Tools for Traffic Control Signals and Devices (NTCIP and Security) Phase 2.*		5. Report Date *February 2, 2015* 6. Performing Organization Code
7. Author(s) *Leonard J. Tung*		8. Performing Organization Report No.
9. Performing Organization Name and Address *Florida State University* *Tallahassee, FL 32306*		10. Work Unit No. (TRAIS) 11. Contract or Grant No. *BDV30-977-05*
12. Sponsoring Agency Name and Address Florida Department of Transportation 605 Suwannee St. MS 30 Tallahassee, Florida 32399		13. Type of Report and Period Covered Final Report 14. Sponsoring Agency Code
15. Supplementary Notes Prepared in cooperation with the USDOT and FHWA		

16. Abstract

Through a coordinated effort among the electrical engineering research team of the Florida State University (FSU) and key Florida Department of Transportation (FDOT) personnel, an NTCIP-based automated testing system for NTCIP-compliant ASC has been developed and constructed. The testing system developed consists of the following:

A laptop running Window 7 operating system with proper ports and software,
A total of 20 NTCIP-based automated testing programs covering all the functionalities of an NTCIP-compliant ASC,
An executable C# Windows Console application to execute all the automated testing programs: *NTCIP_TEST2.exe*, and
A user manual for the NTCIP-based automated ASC testing system.

In the area of security for traffic control systems, extensive literature search has been conducted. A set of guidelines detailing the Best Practices for the Security of Traffic Control Systems has been developed.

17. Key Word	18. Distribution Statement
ASC, NTCIP, Automated Testing Programs, C# language, Security	No restriction.

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	18	

ACKNOWLEDGEMENTS

The authors would like to express their sincere appreciation to Jeffrey M. Morgan, Carl A. Morse, and Matthew Dewitt of the Florida Department of Transportation for the guidance and support that they provided on this project.

EXECUTIVE SUMMARY

It has been a goal of the Traffic Operation and Research Office at Florida Department of Transportation (FDOT) to develop an adequate testing system enabling key personnel at FDOT to conduct comprehensive testing of Actuated Signal Controllers (ASC) submitted by various manufacturers/vendors for certification. The past efforts have led to testing systems which are manufacturer dependent due to the lack of a standard protocol for the communications of traffic control systems. The development and the eventual adoption of National Transportation Communications for ITS (Intelligent Transportation Systems) Protocol (NTCIP) have made possible of an NTCIP-based automated testing system that is manufacturer independent.

Through a coordinated effort among the electrical engineering research team of the Florida State University (FSU) and key Florida Department of Transportation (FDOT) personnel, an NTCIP-based automated testing system for NTCIP-compliant ASC has been developed and constructed. The testing system developed consists of the following:

A laptop running Window 7 operating system with proper ports and software,
A total of 20 NTCIP-based automated testing programs covering all the functionalities of an NTCIP-compliant ASC,
An executable C# Windows Console application to execute all the automated testing programs: *NTCIP_TEST2.exe*, and
A user manual for the NTCIP-based automated ASC testing system.

In the area of security for traffic control systems, extensive literature search has been conducted. A set of guidelines detailing the Best Practices for the Security of Traffic Control Systems has been developed.

This report contains the NTCIP-based Automated ASC Testing Device User Manual, the source codes of the testing software, and the Best Practices for the Security of Traffic Control Systems which have been developed during the current research project. All the results and products of this research project are compiled and stored in the accompanying compact disc (CD) or via the projects web site at: http://eng.fsu.edu/~tung/terl/index.htm.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ABBREVIATIONS

Abbreviation	Full Description
ANTS	Alternative NTCIP Testing Software
APL	Approved Product List
ASC	Actuated Signal Controller
ATIU	Automated Testing Interface Unit
BIU	Bus Interface Unit
CD	Compact Disc
CID	Controller Interface Device
CORSIM	Corridor Simulation
COTS	Commercial-off-the-shelf
ESCC	Enhanced Serial Communication Controller
EW	East-West bound
FDOT	Florida Department of Transportation
FSU	Florida State University
ITS	Intelligent Transportation Systems
MMU	Malfunction Management Unit
NEMA	National Electrical Manufacturers Association
NS	North-South bound
NTCIP	National Transportation Communications for ITS Protocol
PC	Personal Computer
PCB	Printed Circuit Board
PED	Pedestrian
PI	Principal Investigator
SBC	Single Board Computer
SDLC	Synchronous Data Link Control protocol
SNMP	Simple Network Management Protocol
SYN	Synchronized
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TERL	Traffic Engineering Research Lab
TSIS	Traffic Software Integrated System
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network

I. Introduction

I.1. Background

As required in Section 316.0745 of the Florida Stature, the Florida Department of Transportation (FDOT) must certify all traffic control signals and traffic control devices as meeting Federal and State standards and specifications. The current methodology used for the testing of certain traffic control signals and devices, such as traffic controllers, involves "suitcase testers" and is extremely time consuming and is not as systematic as it could be. Among the findings of the previous research project was the need to investigate the addition of other test capabilities that would allow the testing of Florida's National Transportation Communications for ITS Protocol (NTCIP) requirements and to investigate possible security issues with the traffic controller.

The traffic signal controller is basically **a microcomputer** located at the intersection that processes various inputs and triggers outputs that control traffic signals, pedestrian signals, and other electronic devices that comprise a signalized intersection. The devices controlled by an Actuated Signal Controller (ASC) include signaling and detecting devices that are within a cabinet located in an intersection. There are three of interface units between the ASC and the controlled devices, including Malfunction Management Unit (MMU), Terminal Facility Bus Interface Units (BIUs), and Detector BIUs.

In an NTCIP framework, the communication between two control centers is carried by a wide area network (WAN) that runs over IP protocols. Similarly, the communications between a control center and an ASC and between two ASCs can be also fulfilled by a WAN, depending on the distances in-between and the networking technology deployed for the communications. However, the communications between an ASC and other devices located in the same intersection are carried by a local area network (LAN) that runs over Ethernet protocols. In general, there are many different variations of the Ethernet protocols available for connecting the ASC to the local devices. For industrial control and automation purpose, one major category is the so-called real-time Ethernet (rtE) that meets the strict timing requirement between a controller such as ASC and its controlled devices such as the signaling detectors and lights. Before moving forward to the NTCIP compatible protocols in the future, the current practice is still using the widely deployed synchronous data link control (SDLC) protocol between the ASC and its controlled devices, due to a very large amount of legacy equipment that have been deployed in the intersections all over the states.

ASC manufacturers typically use proprietary software and hardware in the design of ASC. There are discrepancies among the manufacturers in their interpretations of many of the ASC specifications. Consequently, the Automated Testing Tools developed by researchers so far are manufacturer dependent. The development and the eventual adoption of NTCIP has demonstrated the possibility of an NTCIP based autonomous testing system which is manufacturer independent and can make the most out of previously NTCIP ASC testing procedures developed at FDOT Traffic Engineering Research Lab (TERL).

In addition, the network security has recently become a national concern over many critical infrastructures. Accordingly, the security of the communications among various ITS elements becomes a major concern within the NTCIP framework. As an example, in the current protocol stacks, the control centers and ASCs within a city are connected by TCP/IP with delay

constrained. For the network level security, there are many solutions available for the security among the ASCs over the communication network due to the rapid progress in networking technology, including authentication and message integrity protocols.

There is inadequate research on the security of the SDLC protocols. For a long SDLC link that goes between a primary network device and many of its secondary devices, such as an IBM mainframe computer and many of its terminals, a common solution is to choose a virtual private network (VPN) to connect the mainframe and its terminals. The SDLC protocol can be then run on top of the VPN connection. However, for a short SDLC link that goes between a primary device and many secondary devices, e.g., the ASC and its controlled devices, i.e. traffic detectors and signal lights, the VPN solution is not viable. One reason is that many secondary devices in ITS are not communicable, i.e., not network devices. Another reason is that there is no economically viable solution to replace all the SDLC related devices immediately. The SDLC, as a legacy protocol, is still being widely used in traffic control systems, although replaced by many of its successors such as HDLC in the other networking industries.

This unique situation requires DOT to conduct research on the security issues associated with the ASC and its controlled cabinet devices, instead of relying on the progress in other communication industries.

I.2. Research Objectives and Supporting Tasks

In the area of autonomous testing for ASC, the main objective is to develop an NTCIP based testing system which combines previously NTCIP test procedures developed at FDOT Traffic Engineering Research Lab (TERL) and the Automated Testing Tools developed at TERL previously.

In the area of security, the main objective is to identify the possible security issues within the traffic control system and provide a set of solutions that can be used to enhance the security of the traffic control systems against FDOT technical requirements as follows:

- First, this project plans to identify the major threats to an ASC system, including man-in-middle attacks, data tampering, bogus commands, and possible attacks, etc.
- Then, the project also plans to develop an architecture for the network that supports a secure traffic control systems, among multiple ASCs and between an ASC and its controlled devices, including authentication, data integrity, and confidentiality.
- Within such architecture, the major possible solutions to address the security issues will be proposed. More specifically, the major encryption and decryption algorithms will be identified.
- The applicable hardware and software framework will be designed to support such added security functions.
- After that, a prototype of secure traffic control system will be built to prove the concept so that the effectiveness of the proposed solutions can be demonstrated.
- Finally, an improved prototype will be tested with the lab equipment in the FDOT-TERL.
- Test results and documents including hardware and software will be submitted to TERL.

To achieve this objective, the following tasks have been proposed in a previous research project, *BDK83-977-20*, titled "Development of Automated Testing Tools for Traffic Control Signals and Devices (NTCIP and Security)".

- Research and review of past efforts applicable to this project.
- Research, review, and selection of existing Commercial-off-the-shelf (COTS) products required for this project.
- System requirements development.
- System design and design reviews.
- System implementation.
- System testing and validation.
- Implementation of production test environment.
- Documentation.
- Training.

The first 4 tasks have been completed in the project, *BDK83-977-20*, and the remaining tasks had been partially carried out in that project and have been completed in this project, *BDV30-977-05*, titled "Development of Automated Testing Tools for Traffic Control Signals and Devices (NTCIP and Security) Phase 2".

II. Literature Review

For the development of an NTCIP-based Automated Testing System for NTCIP-compliant ASCs, the following standards have been studied and complied with:

NTCIP 1201 - NTCIP Global Object (GO) Definitions
NTCIP 1202 - NTCIP Object Definitions for ASC
NTCIP 8007 - Testing and CA Documentation within NTCIP Standards
ATC Controller Standard Revision 5.2a

For the development of the guidelines detailing the Best Practices for the Security of Traffic Control Systems, an extensive literature search has been conducted. A list of all the references is given the reference section.

III. Areas of Work and Scope

The key areas of work alongside their scopes are listed in Table 1.

Table 1: Areas of Work and Scope

Area of Work	Scope
System implementation.	The PI and his staff will be responsible for implementing the system as outlined in the design phase. This will include, but not be limited to, producing code to modify the existing protocols and implement security primitives including necessary node authentication, message integrity, and digital signature for important control commands. All test procedures created shall follow the format outlined in NTCIP 8007.
System testing and validation.	The PI and his staff will be responsible for thoroughly testing the system in order to identify any design flaws or bugs within the system. If design flaws are found, the team shall modify the design, implement the design changes, and retest the system. If bugs are discovered, the team shall isolate and correct the bugs and retest the system to verify proper operation.
Implementation of production test environment.	The PI and his staff will be responsible for packaging the test software into an installer that can be easily distributed. The PI and his staff will demonstrate to FDOT that the installer can be used to easily create a production test environment on a "clean" PC target (PC should only possess a clean installation of Windows XP Professional or a compatible Windows operating system).
Documentation.	The PI and his staff will be responsible for creating support and design documentation. This will include, but is not limited to, a user manual for the final packaged system (including software installation, operation, and hardware setup), flow charts detailing software module interactions and software design concepts, and comments within the source code to make it easy for someone other than the programmer to understand how the code works.
Training.	At no additional cost to FDOT, the PI and his staff will be responsible for providing up to 80 hours training to various FDOT employees on how to install, configure, and operate the final system, as well as comprehend the output from the various tests developed. Training will be conducted at the FDOT-TERL in Tallahassee, Florida.
Draft and Final Report.	Ninety (90) days prior to the end date of the task work order, the university will submit a draft final report to sandra.bell@dot.state.fl.us The draft final report will contain a disclaimer, a summery, a Technical Report Documentation Page and the source codes developed for the automated testing system. The draft final and final reports must follow the Guidelines for University Presentation and Publication of Research available at http://www.dot.state.fl.us/research-center/Project_Mgt_Resources.shtm The report must be well-written and edited for technical accuracy, grammar, clarity, organization, and format.

IV. Results and Products

All the results and products of this research project are compiled and stored in the accompanying compact disc (CD). The summary of results and products is presented in Table 2.

Table 2: Results and Products

Area of Work	Scope
System implementation.	A package of the testing software and its installer has been developed. The package permits the installation of the testing software on a laptop running the operation system of Window 7 and the Sequel Server 2012 Express. The testing software consisting of 20 NTCIP-based automated testing programs covering all the functionalities of an NTCIP-compliant ASC (in the accompanying CD).
System testing and validation.	A series of testing have been performed on 5 different models of NTCIP-compliant ASC by various manufacturers. Sample testing reports for prevalent traffic scenarios at an intersection with such an NTCIP-compliant ASC have been generated.
Implementation of production test environment.	An executable C# Windows Console application to execute all the automated testing programs: *NTCIP_TEST2.exe* (in the accompanying CD) has been installed on a Laptop running Window 7.
Documentation.	NTCIP-based Automated ASC Testing Device User Manual (in the accompanying CD). Testing Software (in the accompanying CD). Best Practices for the Security of Traffic Control Systems (in the accompanying CD).
Training.	The training sessions were about 4 hours per week, either on Monday or on Wednesday, started on 10/6/2014 and ended on 12/15/2014. The training was conducted by Yizhou Dong.
Draft and Final Report.	Final report on CD in Web format.

V. Conclusion

The FSU electrical engineering research team and key FDOT personnel have developed an NTCIP-based Automated Testing System for NTCIP-compliant ASCs. This testing system is manufacturer/vender independent.

In the area of security for traffic control systems, extensive literature search has been conducted. A set of guidelines detailing the Best Practices for the Security of Traffic Control Systems is developed.

References

1. NTCIP 1201 - NTCIP Global Object (GO) Definitions, http://www.ntcip.org/library/documents/
2. NTCIP 1202 - NTCIP Object Definitions for ASC, http://www.ntcip.org/library/documents/
3. NTCIP 8007 - Testing and CA Documentation within NTCIP Standards, http://www.ntcip.org/library/documents/
4. ATC Controller Standard Revision 5.2a, http://www.ite.org/standards/atc/
5. Econolite ASC/3 user manual. (n.d.). Retrived March 15th, 2014 from http://www.econolite.com/Products/controllers/asc-3.aspx
6. Siemens M-50 series user manual. (n.d.). Retrived March 15th, 2014 from http://www.rgatraffic.com/pdf/siemens_controller_line_for_use_in_nema_style_cabinets_m50_series_traffic_controller.pdf
7. MaCain eX NEMA user manual. (n.d.). Retrived March 15th, 2014 from http://controlspecialists.com/images/epacm50.pdf
8. Peek ATC 1000 user manual. (n.d.). Retrived March 15th, 2014 from http://www.ustraffic.net/atc_1000.php
9. Intelight 2070 LDX user manual. (n.d.). Retrived March 15th, 2014 from http://www.intelight-its.com/product/controllers/item/3-intelight-controller-model-2070l.html
10. Trafficware ATC 2070 user manual. (n.d.). Retrived March 15th, 2014 from http://www.trafficware.com/wp-content/uploads/2013/08/ATC-Traffic-Controller.pdf
11. Insignares, M. (2005). NTCIP CORBA Security Service Specification 1105.
12. Ragsdale, P. (2007). NTCIP Object Definitions for ASC 1202 v02.
13. Denney, R. (2010). NTCIP Object for Signal System Masters 1210.
14. http://www.wired.com/science/discoveries/news/2005/08/68507
15. http://latimesblogs.latimes.com/lanow/2009/12/engineers-who-hacked-in-la-traffic-signal-computers-jamming-traffic-sentenced.html
16. http://articles.latimes.com/2007/jan/09/local/me-trafficlights9
17. http://hackaday.com/2012/06/13/traffic-signal-controller-pulls-data-over-wifi/
18. http://www.cyberwarzone.com/hack-traffic-lights-cisco-equipment-future
19. U.S. Department of Transportation ITS Joint Program Office-HOIT. Intelligent Transportation Systems (ITS) Standards Program Strategic Plan for 2011 -- 2014.
20. Directorate-General for Mobility and Transport. Intelligent transport systems in action : action plan and legal framework for the deployment of Intelligent Transport Systems (ITS) in Europe. 2013.
21. U. of Missouri/MoDOT. Best Practices in ITS Equipment Procurement. 2013.

22. SNMP Research International, Inc. SNMP research white paper. http://www.snmp.com/snmpv3/v3white.shtml

23. Herrick, G. C. (1999). THE NTCIP GUIDE: NATIONAL TRANSPORTATION COMMUNICATIONS FOR ITS PROTOCOL (VERSION 2 DRAFT) (No. NTCIP 9001 v02. 05).

24. ESET. Internet Security White Paper. http://www.eset.com/us/resource/papers/white-papers.2013

25. SNMP v3 website. https://www.ibr.cs.tu-bs.de/projects/snmpv3/

Appendix A

NTCIP-based Automated ASC Testing Device User Manual

By

Yizhou Dong

Department of Electrical and Computer Engineering
Florida State University

Appendix B

Best Practices for the Security of Traffic Control Systems

By

Huipu Fan and Ming Yu

Department of Electrical and Computer Engineering
Florida State University